IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) A method of generating a password for at least one application using a single key, said method comprising the steps of:

receiving said single key by a password generator;

receiving a first application name by the password generator at a first time, wherein the first application name is associated with a first application;

receiving a first user selection specifying that no time period applies in the generating of a password by the password generator;

generating a first instance of a first password for said first application by the password generator, wherein the generating of the first instance of the first password is based on at least said first application name received at the first time and based on said single key;

receiving said first application name again by the password generator at a second time; ~~and~~

receiving a second user selection after the second time specifying that no time period applies in the generating of a password by the password generator;

generating a second instance of the first password for said first application by the password generator, wherein the generating of the second instance of the first password is based on at least said first application name received at the second time and based on said single key, and the generated first password is identical in its first and second instances; ~~if a time interval has~~

~~been user specified but has not elapsed between the first and second times and if no time interval has been user specified for the first and second instances.~~

receiving said first application name again by the password generator at a third time;

receiving a third user selection after the third time specifying that a first time period applies in the generating of a password by the password generator;

receiving a user specification of the first time period; and

generating a third instance of the first password for said first application by the password generator, wherein the generating of the third instance of the first password is based on at least said first application name received at the third time and based on said single key, wherein if the third time is after the second time by less than the specified first time period the generated first password is identical in its first, second and third instances.

2. (currently amended) The method according to claim 1, comprising the further steps of:

receiving a second application name by the password generator at a fourth ~~third~~ time, wherein the second application name is different than the first application name and is associated with a second application;

generating a first instance of a second password for said second application by the password generator, wherein the generating of the first instance of the second password is based on said second application name received at the third time and based on said single key, wherein the second password is different than the first password;

receiving said second application name again at a fourth time by the password generator; ~~and~~

receiving a fourth user selection after the fourth time specifying that no time period applies in the generating of a password by the password generator;

generating a second instance of the second password for said second application by the password generator, wherein the generating of the second instance of the second password is based on at least said second application name received at the fourth time and based on said single key and the generated second password is identical in its first and second instances; ~~if a time interval has been user specified but has not elapsed between the first and second times and if no time interval has been user specified for the first and second instances.~~

receiving said first application name again by the password generator at a fifth time;

receiving a fifth user selection after the fifth time specifying that a second time period applies in the generating of a password by the password generator;

receiving a user specification of the second time period; and

generating a third instance of the second password for said second application by the password generator, wherein the generating of the third instance of the second password is based on at least said second application name received at the fifth time and based on said single key, wherein if the fifth time is after the fourth time by more than the specified second time period the generated second password is different in its third instance than in its first and second instances.

3. (currently amended) The method according to claim 1, comprising the further steps of:

~~receiving a user specified time interval by the password generator indicating an interval during which the password generator is to produce identical instances of the first password for identical instances of the received first application name and single key; and~~

~~generating a third instance of the first password responsive to receiving said application name at a time after expiration of the interval, wherein in the third instance the generated first password is different than the first and second instances of the first password, even though the application name received for generating the third instance of the first password is identical to the application name received at the first and second times.~~

receiving said first application name again by the password generator at a fourth time;

receiving a fourth user selection after the fourth time specifying that a second time period applies in the generating of a password by the password generator;

receiving a user specification of the second time period; and

generating a fourth instance of the first password for said first application by the password generator, wherein the generating of the fourth instance of the first password is based on at least said first application name received at the fourth time and based on said single key, wherein the fourth time is after the third time by more than the specified second time period, so that the fourth instance of the generated first password is different than at least its first and second instances.

4. (canceled)

5. (original) The method according to claim 1, wherein generating said first password utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

6. (original) The method according to claim 1, comprising the further step of:

generating a first userid for said first application, based on at least said single key and said first application name.

7. (original) The method according to claim 6, comprising the further step of:

receiving a first userid time period;

wherein generating said first userid is further based on said first userid time period.

8. (original) The method according to claim 6, comprising the further step of:

receiving first userid constraints for said first userid;

wherein generating said first password is further based on said first userid constraints.

9. (original) The method according to claim 6, wherein generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

10. (original) The method according to claim 1, wherein said first application is selected from the group of applications consisting of bank account, Internet email account, Internet website, and computer account.

11-35. (canceled)